

Android: za inficirane aplikacije spremni! (2/2)

čet, 2018-01-25 09:36 - Ratko Žižek



U prethodnom smo članku sveli točku 6 na napomenu: "Cyber kriminalci imaju nezgodnu navadu plasirati nekoliko čistih verzija aplikacije, onda počnu distribuirati istu aplikaciju "obogaćenu" malwareom. Srećom, nismo nemoćni ali treba znati kontrirati." Slijedi razrada 6. točke.

Bitna značajka raznih vrsta digitalnih nametnika - trojanaca, spywarea, keyloggera... - jest potreba spajanja na određene javne IP adrese kako bi kontaktirali "maticu", usput predali naše podatke ili primili naredbu. Zato ćemo svoj smartfon naoružati alatima za praćenje rada aplikacija i mrežnog prometa. Kako to već biva u praksi, što više pozornosti im posvetimo to bolje ćemo kontrolirati svoj uređaj. Puno dopunskih informacija o vanjskim IP adresama i URL-ovima časkom ćemo prikupiti s Weba, dobra polazna točka je <https://www.malwareurl.com/>, uostalom, vidjet ćemo da nam neki od sistemskih alata nude preusmjeravanje na neki anti*.* web servis kako bismo nastavili s istraživanjem.

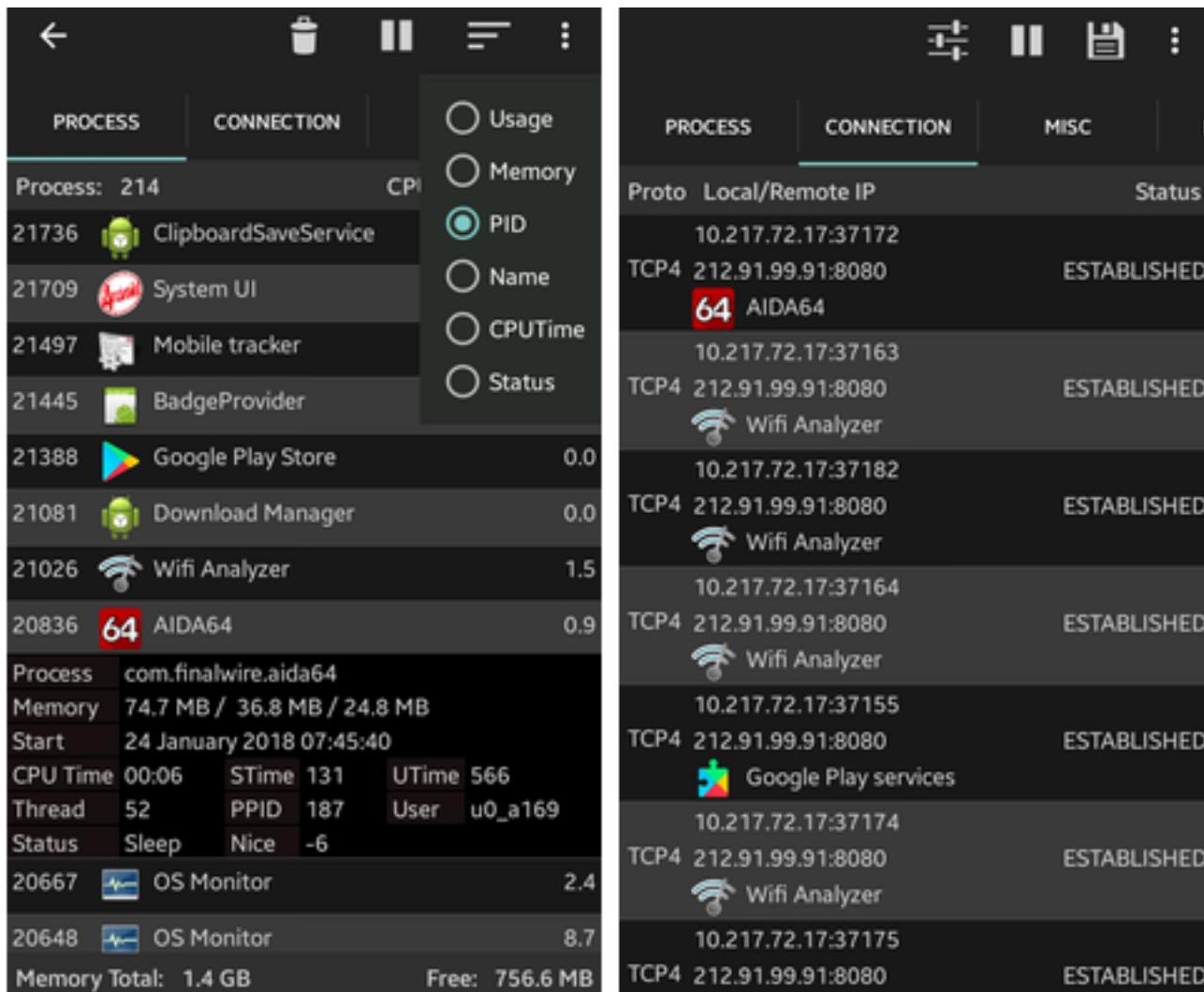
Sljedećih par napomena o tipičnom ponašanju Android aplikacija i dozvolama AOS-a verzije Nougat/Oreo pomoći će nam u obrani suvereniteta našeg digitalnog suradnika, time i nas samih.

a) Budući da je tako od samih početaka, danas možemo ustvrditi da je za AOS aplikacije normalno "istrčavati" na Internet. To radi većina predstaliranih i naknadno instaliranih aplikacija, svaka ima neke svoje okidače i razloge za takvo ponašanje. Možebitnih razloga je puno i uglavnom se smatraju legitimnima - od "cicanja" reklama (tipično za besplatne inačice aplikacija) do informiranja Googleovih servisa o stanju sustava, lokaciji uređaja, našim navikama... ma znate to već, bitno nam je ovo:

- Svakoj je aplikaciji defaultno dopušteno trošenje podatkovne veze u pozadini, znači, aplikaciju ne moramo pokrenuti niti moramo biti na bežičnoj mreži da bi kontaktirala neki vanjski server/servis.
- Neke aplikacije odjurit će "vanka" kad ih pokrenemo, ali postoje i one koje se povremeno samopokrenu u pozadini, popričaju s udaljenim serverom a onda se ili opozovu ili ostanu aktivne kao pozadinski proces.

Poanta: Ne postoji lako uočljiv, jednoznačan indikator koji će upućivati na prisutnost zločudnog koda niti ga je lako sprječiti u prijenosu podataka ili primanju instrukcija. Kad se, recimo, legitimna aplikacija ne bi mogla ponašati po modelu "sama se pozovem - sama se opozovem" imali bismo dobar kriterij za razlikovanje i daljnje postupanje. No, stanje je takvo kakvo jest i s time moramo računati.

b) AOS verzije Nougat uveo je razne sigurnosne inovacije s ciljem što bolje međusobne izolacije aplikacija i AOS-a od utjecaja aplikacija. Nuspojava je blokiranje svih sistemskih alata usmjerenih ka praćenju procesa i sistemskih logova, to smo već spomenuli u 1. točki teme. Hvalevrijedni programski uratci poput OS Monitora na Nougatu su beskorisni osim ako je uređaj rootan a potonje, podsjećam, ne želimo jer time povećavamo mogućnost probroja u sustav. Budući da postoje napadi u kojima malware djeluje kao proces sasvim nevidljiv na razini korisničkog sučelja, ili se čak ugnježduje u neki postojeći legitimni proces, bez alata za analizu procesa značajno nam je otežano otkrivanje uljeza, dovoljno je pogledati nižu sliku da shvatimo kakve smo dragocjene pomagače izgubili.



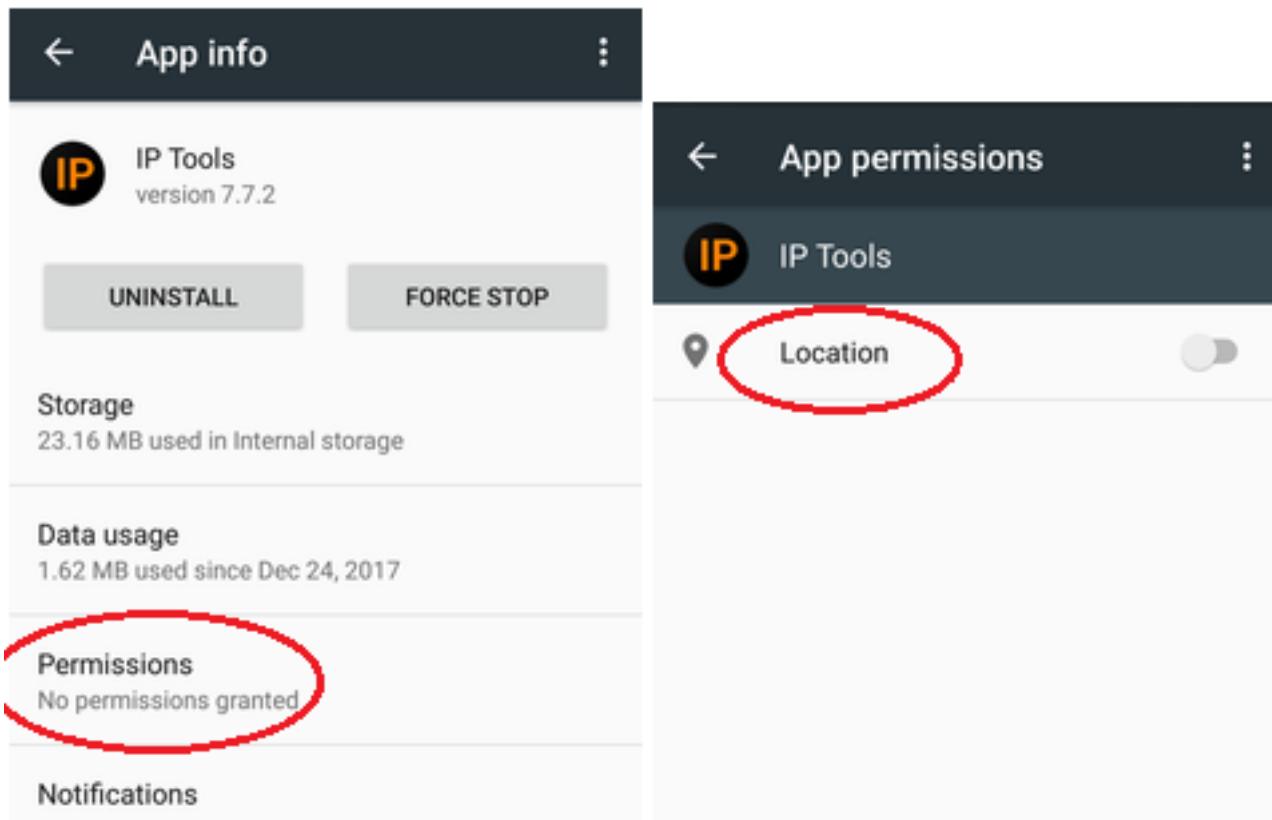
The screenshot shows two main sections of the AIDA64 application. On the left, a list of processes is displayed with columns for Process ID, Application icon, Process name, CPU usage, and RAM usage. A context menu is open over the row for process 21736, 'ClipboardSaveService'. The menu options are: Usage, Memory, PID (which is selected), Name, CPUPTime, and Status. Below this, detailed system information is shown: Process com.finalwire.aida64, Memory 74.7 MB / 36.8 MB / 24.8 MB, Start 24 January 2018 07:45:40, CPU Time 00:06, Thread 52, Status Sleep, and Memory Total: 1.4 GB. On the right, a list of network connections is shown with columns for Proto, Local/Remote IP, and Status. The connections listed are: TCP4 10.217.72.17:37172 to 10.217.72.17:37163 (Status ESTABLISHED, AIDA64), TCP4 10.217.72.17:37163 to 10.217.72.17:37182 (Status ESTABLISHED, Wifi Analyzer), TCP4 10.217.72.17:37182 to 10.217.72.17:37164 (Status ESTABLISHED, Wifi Analyzer), TCP4 10.217.72.17:37164 to 10.217.72.17:37155 (Status ESTABLISHED, Wifi Analyzer), TCP4 10.217.72.17:37155 to 10.217.72.17:37174 (Status ESTABLISHED, Google Play services), TCP4 10.217.72.17:37174 to 10.217.72.17:37175 (Status ESTABLISHED, Wifi Analyzer), and TCP4 10.217.72.17:37175 to 10.217.72.17:37176 (Status ESTABLISHED, Wifi Analyzer).

c) Nougat (i Oreo) prakticira automatsko dodjeljivanje dozvola aplikacijama ako te dozvole spadaju u kategoriju "Normal". Tek kad aplikacija zatraži neku dozvolu iz kategorije "Dangerous", AOS izvješćuje korisnika i traži njegov pristanak. Susreli smo se s tim upitima svi mi koji smo se u nekom trenutku dočepali smartfona ili tableta s novijim AOS-om. To je svakako dobra praksa, kao i mogućnost da korisnik po volji upravlja tim opasnim dozvolama - uključuje ih ili isključuje - tijekom životnog ciklusa aplikacije na svom uređaju. Ali za nas su nepovoljna ova dva rješenja:

- Svaka aplikacija - bila ona dobroćudna ili zloćudna - može nesputano koristiti WiFi mrežni podsustav Android uređaja. Dozvole kojima se regulira ponašanje aplikacije u WiFi kontekstu spadaju u kategoriju Normal pa korisnik to ne može regulirati u AOS ugrađenim naredbama.
- Opasne su dozvole grupirane u nekoliko grupa a primjenjuju se tako da se mogu zlorabiti, posebice nakon ažuriranja aplikacije. "Lakoprobavljiv" primer: Postoji grupa dozvola android.permission-group.STORAGE, ona obuhvaća dozvolu za čitanje i dozvolu za pisanje/brisanje po korisničkom dijelu podatkovne memorije. Tijekom instalacije aplikacija zatraži od AOS-a, posredstvom svoje konfiguracijske datoteke AndroidManifest.xml, pravo čitanja podataka, AOS zatraži od nas odobrenje...(itd., to znamo), ali ako naknadno autor u manifest te aplikacije postavi zahtjev za dozvolom "piši/brisi", AOS će to prihvatiti bez notifikacije korisnika. Ovakvim baratanjem dozvolama otvara se manevarski prostor hakeru da neprimjetno osposobi svoj softver za iskorištavanje ranjivosti u sustavu. Kontramjera je povremena kontrola dozvola aplikacija, nije to lako ali je izvedivo jer, vidjet ćemo, postoje alati koji nam olakšavaju taj posao.

Odlično štivo o dozvolama nalazi se na adresi <https://developer.android.com/>, mi ćemo priču o njima

završiti jednom ilustracijom. Sad kad znamo kako su dozvole kategorizirane i kako se primjenjuju, neće nas zbunjivati izvještaj AOS-ovog Application Managera u kojem općepoznati alat IP Tools nema nikakve dozvole a nesmetano radi, kak' sad pa to?! Odgovor je: aplikacija funkcioniра na razini mrežnog podsustava, za to su joj dovoljne dozvole "Normal" a njih joj AOS blagonaklono daruje; jedina Dangerous dozvola (Location) je isključena... u konačnici, ali samo za neupućene u ove fineze, aplikacija radi bez ikakvih dozvola.



Ok, gornje smo "naštrebitali", voljni smo braniti se od svakojakih digitalnih parazita i humanoidnih zločestoba koje iz njih stoje... sad čemo se još naoružati s par odličnih alata. Zajedničko nižim alatima je to što rade bez superuser prava, za aktiviranje svih funkcionalnosti treba kupiti licencu ali, srećom, i besplatna verzija od velike je pomoći. Iskreno, barem što se tiče navedenih alata, trošak na licencu uistinu je zanemariv u odnosu na ono što dobijamo.

* NETWORK CONNECTIONS (Anti Spy Mobile) ukratko: bilježi spajanje lokalnih aplikacija i servisa na vanjske IP adrese; vrijedi i obratno, registrirati će i dolaznu konekciju. Također će pratiti internu komunikaciju aplikacija ako se odvija posredstvom loopback mrežnog adaptera. Pored uvida u detalje konekcije, od IP do geolokacije, daje i kvantitativne podatke o ostvarenom prometu u oba smjera. Posebno su nam zanimljivi opcija *Show notifications when hidden apps are making connections* te izvješće o dozvolama iskorištenim tijekom konekcije, nije teško skontati zašto. Sve što alat hvata možemo snimati, spremiti i potom analizirati. Aplikacija je prilagođena sistemcima u svakom svom aspektu, riječ je o preciznom softverskom instrumentu krcatom mogućnostima.

Niže se bavimo "inspekcijom inspektora", pratimo ponašanje NetGuarda, aplikacijskog vatrozida. Tap-po-tap i pred očima nam se redaju dragocjeni podaci o ponašanju aplikacije i značajkama čvorova s kojima komunicira.

CONNECTIONS	CONNECTIONS LOG	APP NETWORK
Order by Most Active	Order by Last Seen	Order by Package
64.233.166.81:443	Last: 1/15/18 10:49	
Android System	Total Activity: 1s	
192.168.43.1:53	Last: 1/15/18 10:49	
Android System	Total Activity: 1s	
193.0.6.150:80	Last: 1/15/18 10:57	
Android System	Total Activity: 7m 55s	
199.212.0.46:80	Last: 1/15/18 10:57	
Android System	Total Activity: 7m 55s	
172.217.16.200:443	Last: 1/15/18 10:53	
Android System	Total Activity: 1s	
172.217.23.130:443	Last: 1/15/18 11:01	
NetGuard	Total Activity: 9m 31s	
216.58.206.2:443	Last: 1/15/18 11:01	
NetGuard	Total Activity: 4m 45s	
172.217.22.34:443	Last: 1/15/18 11:01	
NetGuard	Total Activity: 4m 45s	
172.217.22.106:443	Last: 1/15/18 10:49	
Google Account Manager	Total Activity: 9m 35s	
216.58.207.46:443	Last: 1/15/18 10:49	
Google Account Manager	Total Activity: 9m 35s	
64.233.166.81:443	Last: 1/15/18 10:49	
Google Account Manager	Total Activity: 2m 25s	

IP Details

172.217.23.130 AS15169
fra16s18-in-f2.1e100.net

IP Administrative Data:

Google LLC (GOOGLE)
1600 Amphitheatre Parkway
Mountain View, CA 94043
United States

IP Geo Location:

Abuse RBL:

There's no abuse data found for this IP/NetBlock.

Apps that are using this IP:

NetGuard	Port: 443
eu.faircode.netguard	Last: 1/15/18 10:57
Google Account Manager	Port: 443
com.google.uid.shared	Last: 1/15/18 10:57

Application Details

NetGuard eu.faircode.netguard ver: 2.169

Permissions granted to this app:

- view network connections
- Allows the app to view information about network connections such as which networks exist and are connected.
- read phone status and identity
- Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call.
- view WLAN connections
- Allows the app to view information about WLAN networking, such as whether WLAN is enabled and name of connected WLAN devices.
- run at startup

IP Addresses used by this app:

172.217.23.130	Port: 443
fra16s18-in-f2.1e100.net	1/15/18 10:59
216.58.206.2	Port: 443
fra16s20-in-f2.1e100.net	1/15/18 10:59
172.217.22.34	Port: 443
fra15s16-in-f2.1e100.net	1/15/18 10:59

Postoji i IP Connections, jednostavan alat koji prikazuje mrežne konekcije u realnom vremenu, praktičan je za nadzor sve dok nemamo potrebu za nekim posebnim istraživanjima (mada, PRO inačica ima i mogućnost izvoza podataka). Vizualno orijentiranim dušama svidjet će se jednostavni geolokator IP adresa Connect jer značajke mrežnih konekcija prikazuju na mapi svijeta.

* PACKET CAPTURE (Grey Shirts) ukratko - mrežno njuškalo koje opominjujuće odlično odraduje svoj posao. Opominjujuće i odlično - kakva je to uvrnuta kombinacija?! Heh, uočite da alat umije analizirati pakete koji cirkuliraju TLS tunelom, što znači da istu tehniku (man-in-the-middle) može primjeniti i neki spyware... toliko o "sigurnim" HTTPS konekcijama smartfona s web uslugama na Internetu! Alat možemo fokusirati na jednu aplikaciju ili pratiti sve njih. Inače, postoji svestraniji, developerima naklonjeniji alat Debug Proxy, ali dok ga ne kupimo gotovo je neupotrebljiv.

Na nižoj slici usnimili smo vjerodajnicu odaslanu ciljnoj web usluzi https-om, pripremamo se spremiti cijelu komunikaciju u PCAP formatu kako bismo na PC-u analizirali Wiresharkom.

last_viewed_list=501818%2C417253%2C465536%2C517048%2C522695%2C521996%2C501817%2C511234%2C511046%2C511901; SESSIONID=tvvjbcgqfuljsfrt2ehru7si6; _pfbsesid=db4fcd51-0a99-71e9-142c-17d241571ee5; db4fcd51-0a99-71e9-142c-17d241571ee5_pfb_event_nr=1; _hjIncludedInSample=1; _gali=login

Save Upstream(<--)
Save Downstream(--->)
Save Both
Save pcap (highlighted)
URL_ENCODED

_csrf_token=8igXBf82zWYDHd-N10oKKC0JGqfRS#2RFAwTj00niw&target=/prijava&failure_target=/prijava&use_name=zizek.ratko@gmail.com&password=Banank1&remember_me=1&login=

HTTP/1.1 302 Found
Date: Sun, 07 Jan 2018 16:32:02 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: SESSIONID=cgdrnekuk8cmggq0q4dghan8t5; path=/; domain=edigital.hr; HttpOnly
Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private

* ASPOTCAT (Sam Lu) ukratko - na pregledan i razumljiv način upoznaje sa stanjem dozvola za svaku aplikaciju. Alat uspoređuje dozvole deklarirane u AndroidManifest.xml određene aplikacije sa realnim stanjem njenih dozvola u sustavu i informira koje su od zatraženih dozvola aktivne a koje su neaktivne, koje su neopasne a koje opasne... ukratko, pomaže u otkrivanju aplikacija s (pre)velikim ovlastima. Nažalost, izvještaji se ne mogu spremiti, to umanjuje vrijednost alata no, s druge strane, informativan je i dotjeranog sučelja. U praksi ćemo ga vjerojatno kombinirati s AOS-ovim upraviteljem aplikacija kako bismo sumnjivoj aplikaciji "reprogramirali" opasne dozvole ili je se riješili po kratkom postupku, deinstalirali.

Recept "rješiti po kratkom postupku" primijenili smo na aplikaciju Mi Remote - zahvaljujući aSpotCatu shvatili smo da ta aplikacija, po namjeni softverski daljinski upravljač, ima zamalo pa administratorske dozvole na sustav. E, nećeš, razbojniče! :o)

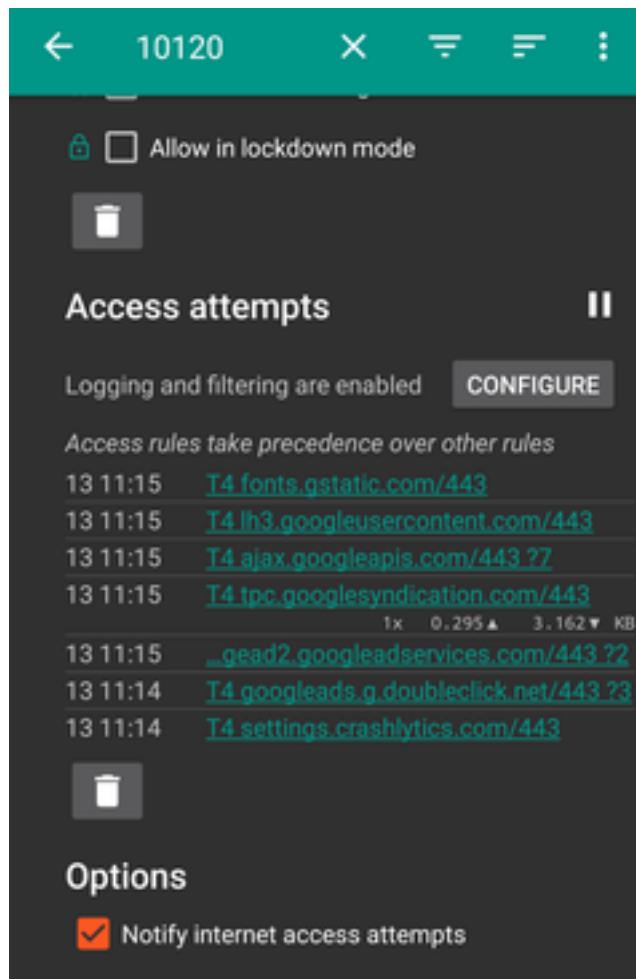
Phone	Contacts	Microphone
...permission-group.PHONE	...ission-group.CONTACTS	...ion-group.MICROPHONE
<ul style="list-style-type: none"> Read phone status and identity Allows the app to access the phone features of the device. This permission allows the app to determine the phone number and device IDs, whether a call is active, and the remote number connected by a call. android.permission.READ_PHONE_STATE protection level is Dangerous 	<ul style="list-style-type: none"> Find accounts on the device Gaping Device Policy Mi Remote Privacy Guard Word 	<ul style="list-style-type: none"> Record audio Allows the app to record audio with the microphone. This permission allows the app to record audio at any time without your confirmation. android.permission.RECORD_AUDIO protection level is Dangerous
Audio Recorder Gaping Device Policy Google Play services Mi Remote NetGuard Privacy Guard Word	Gaping Device Policy Mi Remote Privacy Guard Word	Audio Recorder Gaping Google Play services Mi Remote PitchLab Lite

* NETGUARD NOROOT FIREWALL (Marcel Bokhorst) ukratko - nije baš pravi firewall jer ne sprječava niti ne registrira dolazne konekcije, ali uistinu je moćno pomagalo. Naime, omogućuje nam da svim ili pojedinim aplikacijama blokiramo spajanje na Internet resurse, nadalje, da pratimo komunikaciju aplikacija - korisničkih i sistemskih - sa čvorovima na Internetu. Pri tome alat rabi notificiranje korisnika i/ili logiranje konekcija. Potonja metoda omogućuje naknadnu vrlo detaljnu analizu komunikacije, samo što trebamo nešto malo iskeširati kako bismo otključali tu funkcionalnost.

Za ispravnu uporabu alata važno je znati da jednokratno izvješćuje o svakoj vanjskoj adresi kojoj aplikacija pristupa. Ako ne znamo za taj detalj, učinit će nam se da su nakon nekog vremena aplikacije prestale izlaziti na Internet. Takav način rada alata u stvari je dobar jer lakše uočavamo i ispitujemo konekcije ka novom odredištu. Upravo takve, za dotičnu aplikaciju neuobičajene konekcije i treba pažljivije analizirati jer ih može uzrokovati malware skriven u aplikaciji. Ako, pak, u nekom trenutku želimo snimiti baš sve URL-ove kojima konkretna aplikacija pristupa, odemo u njenu sekciju Access attempts i izbrišemo postojeće zapise.

Kad to zatražimo, Netguard će nas preusmjeriti na uslugu scanadviser.com, gdje možemo provjeriti sigurnosni status adrese/servisa na kojega se neka aplikacija spaja.

Na nižoj slici provjeravamo aSpotCat, fokusirani smo na maloprije spomenutu sekciju Access attempts.



Tijekom nadmudrivanja s aplikacijama i alatima dobro će nam doći "one-tap" alat FAST TASK KILLER, njegov je učinak sličan soft resetu pa nam pomaže da za neku planiranu aktivnost ekspresno

dobijemo okolinu pročišćenu od procesa i podatkovnih struktura kreiranih našim ranijim postupcima.

*

Vaš autor od nedavno ima dva smartfona, etiketirao ih je kao "poslovni" i "prljavi". Na poslovnom su samo neophodne i dobro provjerene aplikacije za internet bankarstvo, kupoprodaju te, dakako, razni sistemski alati; uključene su sve zaštitne funkcije - lokalne i Googlove oblačne - koje se mogu uključiti a da ipak nesmetano rabim taj uređaj. "Prljavac" mi služi za stručnu edukaciju i zabavu, što neizostavno uključuje "landranja" po Webu, istraživanje raznih online sadržaja, instaliranje i ispitivanje svakojakih aplikacija sa svakojakih repozitorija.... i tako to. Tragikomično ali istinito: tek sada, opremljen s dva smartfona, mogu se uistinu koristiti svim prednostima mobilnih uređaja, efikasno ovladavati mobilnim tehnologijama a usput *i spavati snom pravednika!* Dodajmo još da "prljavko" uvelike doprinosi zaštiti svog čistog kolege jer upravo njime stječem dragocjena iskustva i vještine iz područja zaštite Android uređaja. Preporučamo! :-)

Vijesti: [QS](#) [1]

Kuharice: [Android](#) [2]

Kategorije: [Operacijski sustavi](#) [3]

Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: [Android](#) [4]

[malware](#) [5]

[zaštita](#) [6]

[alati](#) [7]

Source URL: <https://sysportal.carnet.hr/node/1792>

Links

- [1] <https://sysportal.carnet.hr/taxonomy/term/10>
- [2] <https://sysportal.carnet.hr/taxonomy/term/64>
- [3] <https://sysportal.carnet.hr/taxonomy/term/26>
- [4] <https://sysportal.carnet.hr/taxonomy/term/183>
- [5] <https://sysportal.carnet.hr/taxonomy/term/214>
- [6] <https://sysportal.carnet.hr/taxonomy/term/204>
- [7] <https://sysportal.carnet.hr/taxonomy/term/215>